Amendments to the Claims

Kindly amend claims 1, 11 & 21 and cancel claims 5-7 & 15-17 (without prejudice) as set forth below. All pending claims are reproduced below, with changes in the amended claims shown by underlining (for added matter) and strikethrough/double brackets (for deleted matter).

1. (Currently Amended) A method of migrating data encrypted using a first key set to data encrypted using a second key set, said method comprising:

performing multiple writes of encrypted data using a first key set;

employing a usage counter to count each use of the first key set to write encrypted data; and

automatically transitioning to a second key set when the count of the usage counter exceeds a defined threshold, the automatically transitioning comprising:

modifying an access table to indicated that encrypted data in a current data location is to be decrypted using the first key set, and is to be re-encrypted using the second key set when undergoing storage to a new data location;

decrypting [[data]] the encrypted data using [[a]] the first key set; [[and]]

re-encrypting, by a data access control function within an integrated system, the data using [[a]] the second key set, wherein the decrypting and the re-encrypting comprise reading the encrypted data from the current data location, decrypting the encrypted data using the first key set, then writing the data as encrypted data to the new data location employing the second key set; and

modifying the access table further with the new data location being defined for encryption and decryption with the second key set.

2. (Original) The method of claim 1, wherein the data access control function comprises a hardware component of the integrated system.

3. (Original) The method of claim 1, wherein the decrypting is also performed by the data access control function of the integrated circuit.

4. (Original) The method of claim 1, further comprising retrieving for decryption, from storage associated with the integrated system, the data encrypted using the first key set.

5. (Canceled).

6. (Canceled).

7. (Canceled).

8. (Original) The method of claim 1, wherein the data encrypted using the first key set is received from a source external to the integrated system.

9. (Original) The method of claim 8, wherein the decrypting is performed in software within the integrated system, and wherein the re-encrypting, by the data access control function, is performed in hardware of the integrated system.

10. (Original) The method of claim 9, wherein the second key set is unique to the integrated system.

11. (Currently Amended) A system of migrating data encrypted using a first key set to data encrypted using a second key set, said system comprising:

means for performing multiple writes of encrypted data using a first key set;

means for employing a usage counter to count each use of the first key set to write encrypted data; and

means for automatically transitioning to a second key set when the count of the usage counter exceeds a defined threshold, the means for automatically transitioning comprising:

means for modifying an access table to indicate that encrypted data in a current data location is to be decrypted using the first key set, and is to be re-encrypted using the second key set when undergoing storage to a new data location;

means for decrypting [[data]] the encrypted data using [[a]] the first key set; [[and]]

means for re-encrypting, by a data access control function within an integrated system, the data using [[a]] the second key set, wherein the decrypting and the re-encrypting comprise reading the encrypted data from the current data location, decrypting the encrypted data using the first key set, then writing the data as encrypted data to the new data location employing the second key set; and

means for modifying the access table further with the new data location being defined for encryption and decryption with the second key set.

12. (Original) The system of claim 11, wherein the data access control function comprises a hardware component of the integrated system.

13. (Original) The system of claim 11, wherein the means for decrypting is also performed by the data access control function of the integrated circuit.

14. (Original) The system of claim 11, further comprising means for retrieving for decryption, from storage associated with the integrated system, the data encrypted using the first key set.

15. (Canceled).

16. (Canceled).

17. (Canceled).

18. (Original) The system of claim 11, wherein the data encrypted using the first key set is received from a source external to the integrated system.

19. (Original) The system of claim 18, wherein the means for decrypting is performed in software within the integrated system, and wherein the re-encrypting, by the data access control function, is performed in hardware of the integrated system.

20. (Original) The system of claim 19, wherein the second key set is unique to the integrated system.

21. (Currently Amended) At least one program storage device readable by a machine embodying at least one program of instructions executable by the machine to perform a method of migrating data encrypted using a first key set to data encrypted using a second key set, said method comprising:

performing multiple writes of encrypted data using a first key set;

employing a usage counter to count each use of the first key set to write encrypted data; and

automatically transitioning to a second key set when the count of the usage counter exceeds a defined threshold, the automatically transitioning comprising:

modifying an access table to indicated that encrypted data in a current data location is to be decrypted using the first key set, and is to be re-encrypted using the second key set when undergoing storage to a new data location;

decrypting [[data]] the encrypted data using [[a]] the first key set; [[and]]

re-encrypting, by a data access control function within an integrated system, the data using [[a]] the second key set, wherein the decrypting and the re-encrypting comprise reading the encrypted data from the current data location, decrypting the encrypted data using the first key set, then writing the data as encrypted data to the new data location employing the second key set; and

modifying the access table further with the new data location being defined for encryption and decryption with the second key set.

* * * * *